(12) UK Patent Application (19) GB (11) 2 341 061 (13) A

(43) Date of A Publication 01.03.2000

(21) Application No 9914053.5

(22) Date of Filing 16.06.1999

(30) Priority Data
(31) 10167928 (32) 16.06.1998 (33) JP

(71) Applicant(s)
NEC Corporation
(Incorporated in Japan)
7-1,Shiba 5-Chome, Minato-Ku, Tokyo, Japan

(72) Inventor(s)
Kenji Kataoka

(74) Agent and/or Address for Service
John Orchard & Co
Staple Inn Buildings North, High Holborn, LONDON,
WC1V 7PZ, United Kingdom

(51) INT CL[7]
G06F 1/00 , H04L 9/32 , H04M 1/66

(52) UK CL (Edition R)
H4P PDCSA
G4A AAP
H4L LEF
U1S S2122

(56) Documents Cited
GB 2335519 A WO 98/07249 A1 WO 97/39553 A1

(58) Field of Search
UK CL (Edition Q) G4A AAP , H4L LECX , H4P PDCSA
INT CL[6] G06F 1/00 12/14 , G08B 13/14 , H04L 9/32 ,
H04M 1/66 , H04Q 7/32 7/38
Online: WPI, EPODOC, JAPIO

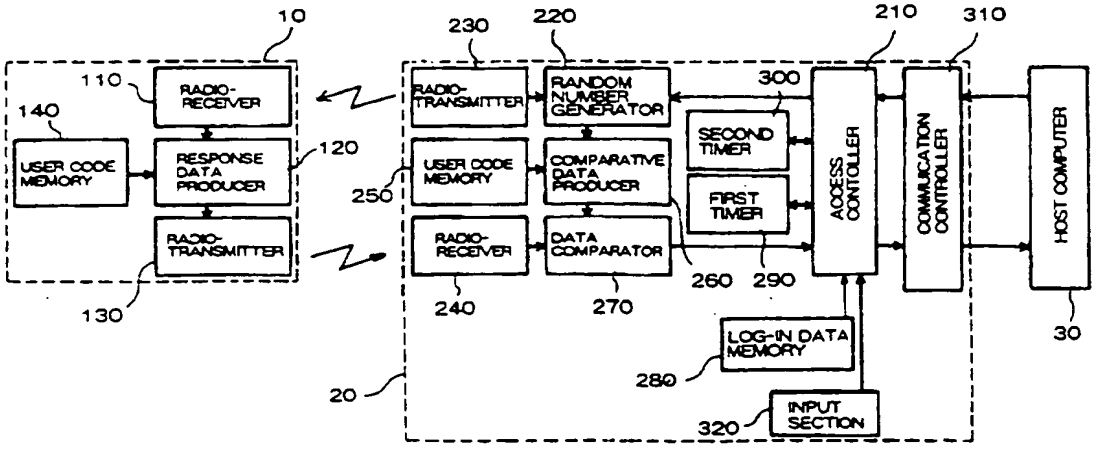
(54) Abstract Title

Portable data communication terminal with separate user authenticating security device in radio communication with the terminal

(57) A portable data communication terminal 20 and an associated user authentication device 10 communicate by radio transceiver means 110,130,230,240. When a user attempts to log the terminal onto a host 30 the terminal sends a challenge to the authenticating device which replies with a coded response. If a correct response is received the users identity is verified and log on is allowed.

In this way the system monitors the proximity of the terminal to the authenticating device to ensure that they are close enough for communication to take place between them before allowing log on. The system may allow a fixed time for responding to the challenge and may periodically challenge the user authenticating device during log on to ensure that the authorised user has not left the terminal unattended while logged on. Also the power of the transmitters may be varied to change the proximity between user and terminal which is required.

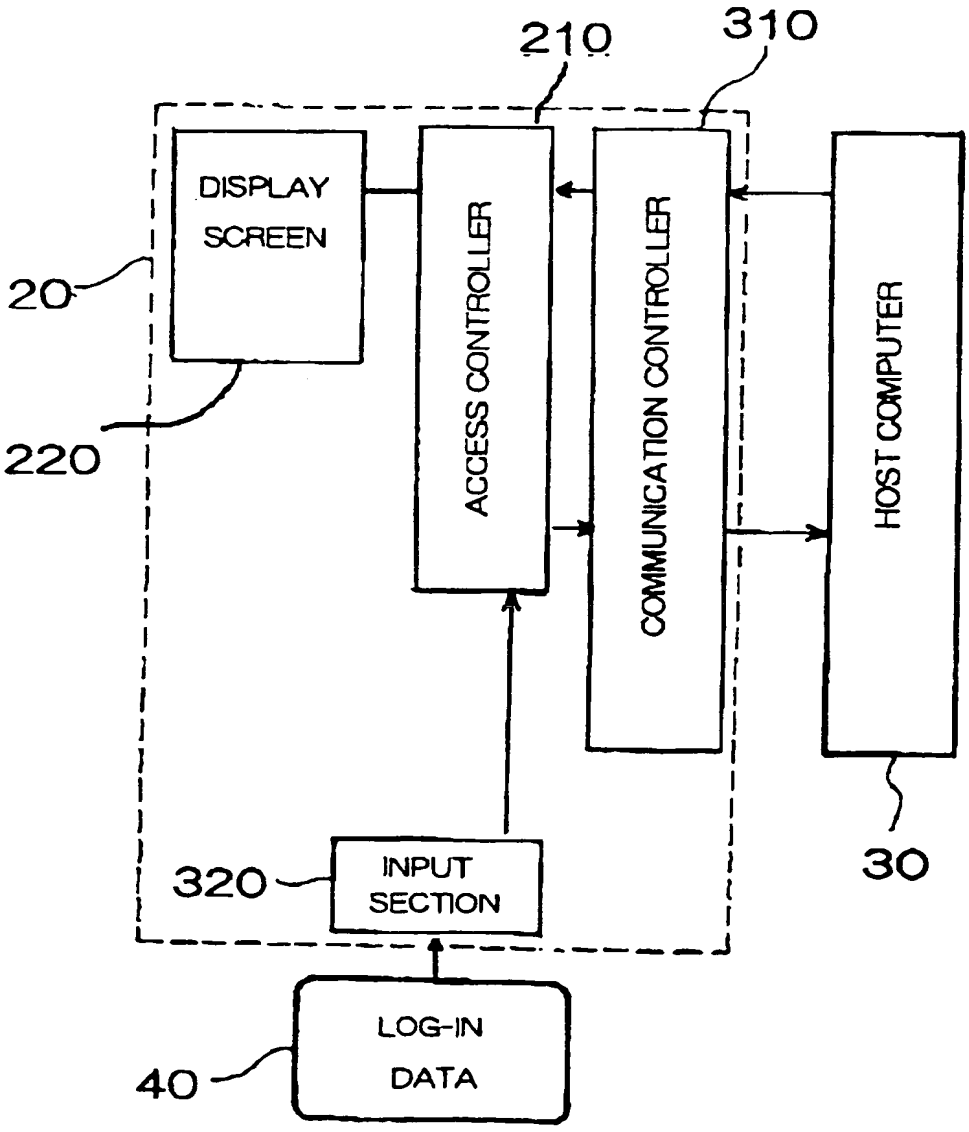
FIG. 2



GB 2 341 061 A

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

FIG.1


210
310
DISPLAY SCREEN
20
220
ACCESS CONTROLLER
COMMUNICATION CONTROLLER
HOST COMPUTER
30
320
INPUT SECTION
LOG-IN DATA
40

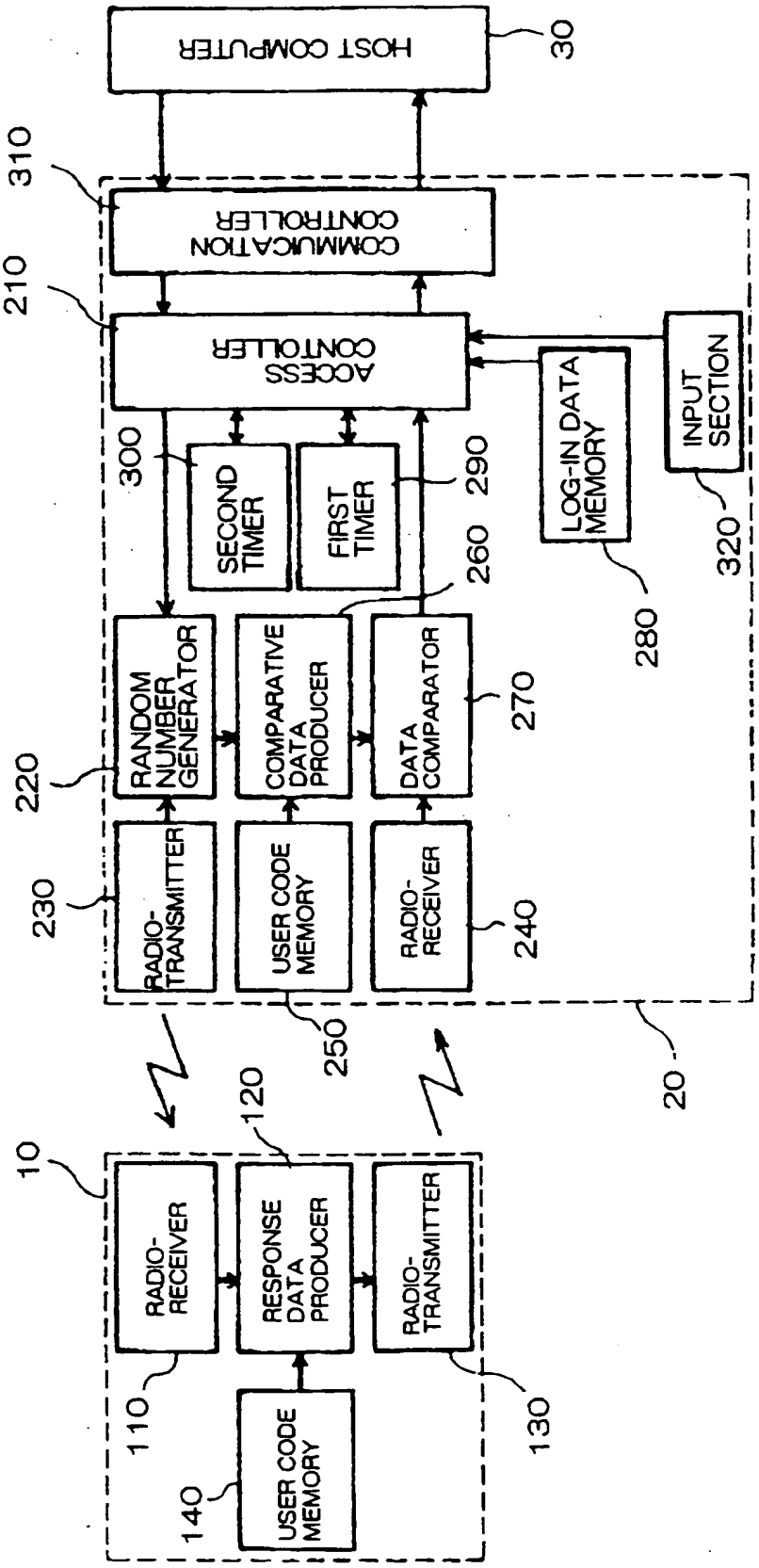

HOST COMPUTER
30
310
COMMUNICATION CONTROLLER
210
ACCESS CONTROLLER
300
SECOND TIMER
FIRST TIMER
290
260
LOG-IN DATA MEMORY
280
INPUT SECTION
320
RANDOM NUMBER GENERATOR
220
COMPARATIVE DATA PRODUCER
DATA COMPARATOR
270
RADIO-TRANSMITTER
230
USER CODE MEMORY
RADIO-RECEIVER
240
250
20
10
120
RADIO-RECEIVER
RESPONSE DATA PRODUCER
RADIO-TRANSMITTER
110
130
140
USER CODE MEMORY

FIG. 2

FIG. 3

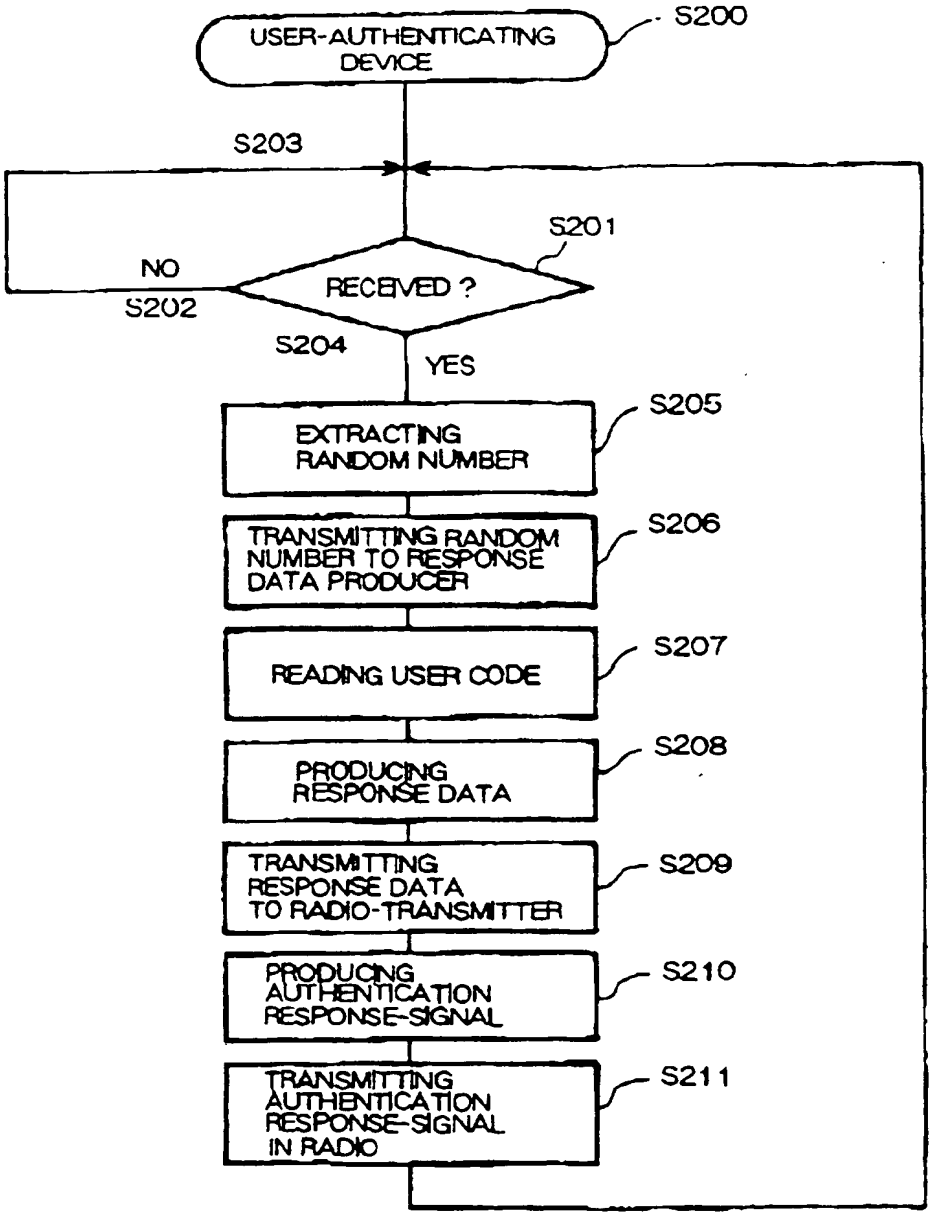

USER-AUTHENTICATING DEVICE
S200
S203
S201
RECEIVED ?
NO
S202
S204
YES
EXTRACTING RANDOM NUMBER
S205
TRANSMITTING RANDOM NUMBER TO RESPONSE DATA PRODUCER
S206
READING USER CODE
S207
PRODUCING RESPONSE DATA
S208
TRANSMITTING RESPONSE DATA TO RADIO-TRANSMITTER
S209
PRODUCING AUTHENTICATION RESPONSE-SIGNAL
S210
TRANSMITTING AUTHENTICATION RESPONSE-SIGNAL IN RADIO
S211

FIG.4

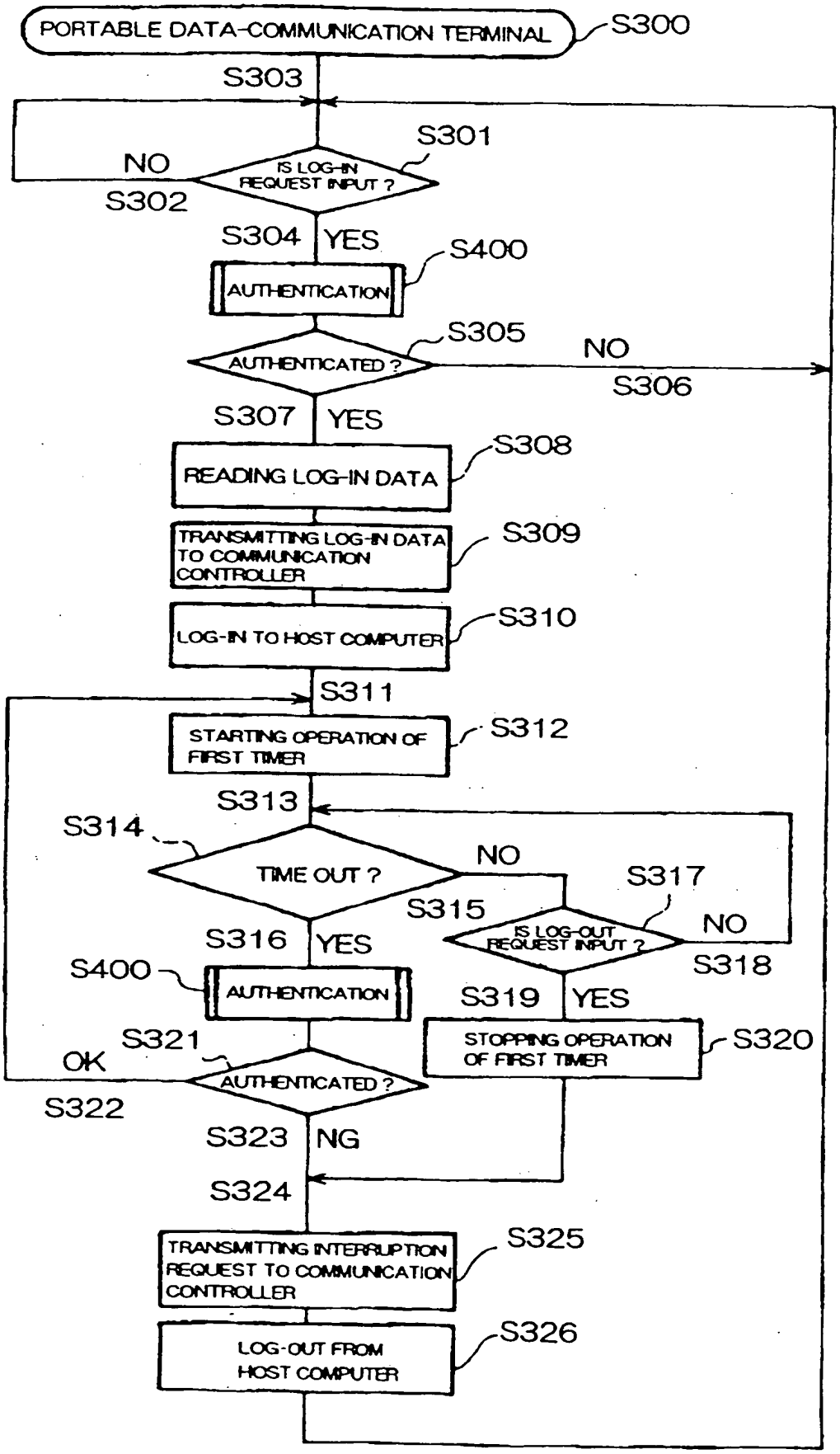
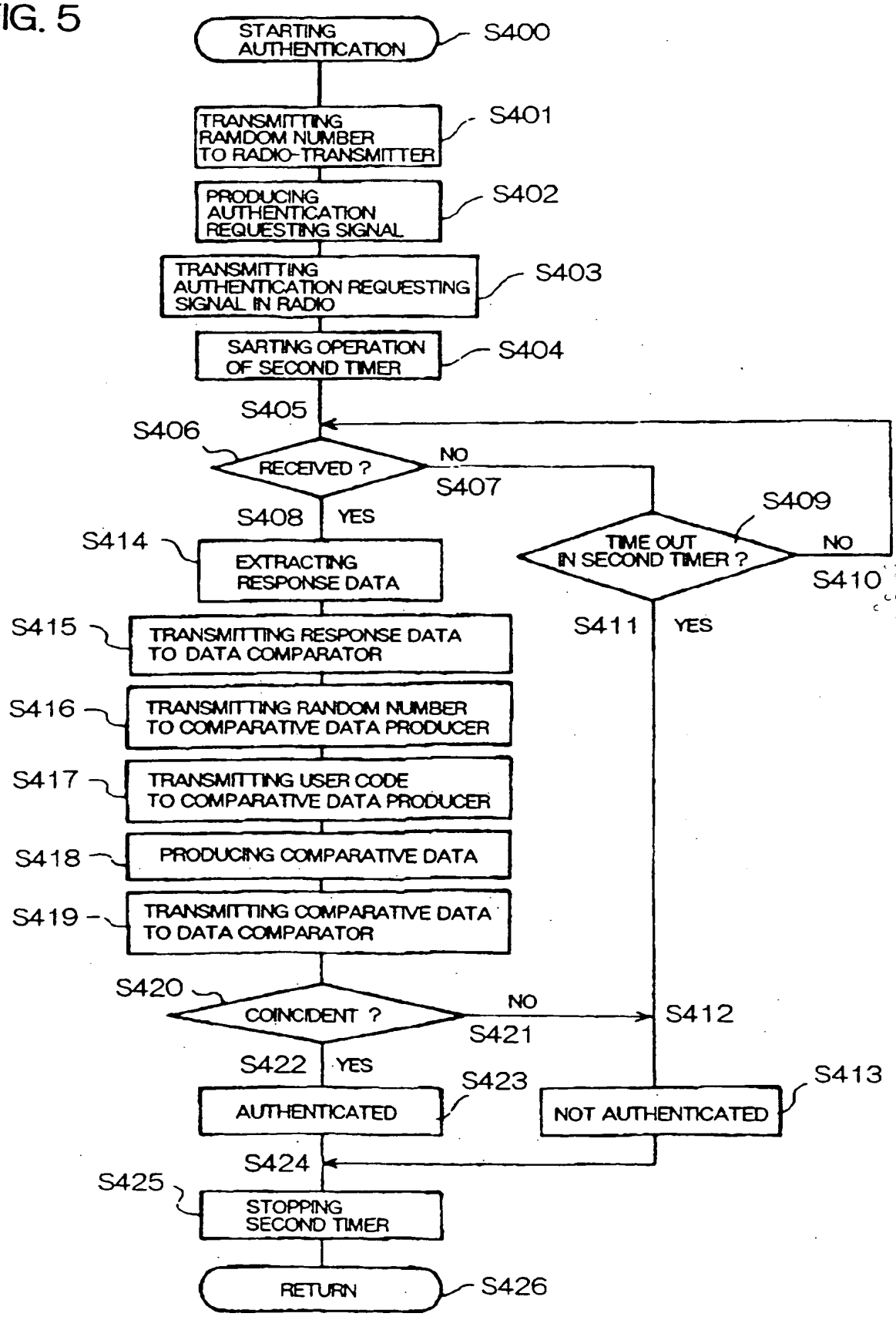

PORTABLE DATA-COMMUNICATION TERMINAL
S300
S303
S301
IS LOG-IN REQUEST INPUT ?
NO
S302
S304
YES
S400
AUTHENTICATION
S305
AUTHENTICATED ?
NO
S306
S307
YES
S308
READING LOG-IN DATA
TRANSMITTING LOG-IN DATA TO COMMUNICATION CONTROLLER
S309
LOG-IN TO HOST COMPUTER
S310
S311
STARTING OPERATION OF FIRST TIMER
S312
S313
S314
TIME OUT ?
NO
S315
S317
IS LOG-OUT REQUEST INPUT ?
NO
S318
S316
YES
S400
AUTHENTICATION
S319
YES
STOPPING OPERATION OF FIRST TIMER
S320
S321
OK
AUTHENTICATED ?
S322
S323
NG
S324
TRANSMITTING INTERRUPTION REQUEST TO COMMUNICATION CONTROLLER
S325
LOG-OUT FROM HOST COMPUTER
S326

FIG. 5


STARTING AUTHENTICATION
S400
TRANSMITTING RAMDOM NUMBER TO RADIO-TRANSMITTER
S401
PRODUCING AUTHENTICATION REQUESTING SIGNAL
S402
TRANSMITTING AUTHENTICATION REQUESTING SIGNAL IN RADIO
S403
SARTING OPERATION OF SECOND TIMER
S404
S405
S406
RECEIVED ?
NO
S407
S408
YES
S409
TIME OUT IN SECOND TIMER ?
NO
S410
S411
YES
S414
EXTRACTING RESPONSE DATA
S415
TRANSMITTING RESPONSE DATA TO DATA COMPARATOR
S416
TRANSMITTING RANDOM NUMBER TO COMPARATIVE DATA PRODUCER
S417
TRANSMITTING USER CODE TO COMPARATIVE DATA PRODUCER
S418
PRODUCING COMPARATIVE DATA
S419
TRANSMITTING COMPARATIVE DATA TO DATA COMPARATOR
S420
COINCIDENT ?
NO
S421
S412
S422
YES
S423
AUTHENTICATED
NOT AUTHENTICATED
S413
S424
S425
STOPPING SECOND TIMER
RETURN
S426

METHOD AND SYSTEM FOR AUTHENTICATING A USER

This invention relates to a method and system for authenticating a user. A method and system to be described below, by way of example in illustration of the invention, relate to use with a portable data-communication terminal.

In previously proposed arrangements, when a data-communication terminal has to log-in to a host computer, the host computer usually asks the data-communication terminal to transmit an account name in order to identify a user and a pass word for use in authenticating a user, as data for use in judging whether a log-in is to be allowed.

Such data-communication terminals have been suggested in the specifications of Japanese Unexamined Patent Publications Nos. 4-233341 and 9-187081.

Reference will now be made to Fig. 1 of the accompanying drawings which is a block schematic diagram of a previously proposed data-communication terminal illustrating a log-in to a host computer.

Referring to Fig. 1, when a data-communication terminal 20 logs-in to a host computer 30, a user is able to input a request for log-in to the data-communication

terminal 20 through an input section 320 of the terminal 20. When a request for log-in is input through the input section 320, an access controller 210 of the data-communication terminal 20 transmits a request for communication to the host computer 30 through a communication controller 310.

When requested by the host computer 30 to show an account name and a password, the access controller 210 informs a user of such a request through a display screen 220 of the data-communication terminal 20. A user receiving such a request is able to input an account name and a password, as log-in data 40, through the input section 320. The thus input log-in data 40 may be transmitted to the host computer 30, and log-in of the data-communication terminal 20 to the host computer 30 is carried out, for instance, when the pass word, as log-in data, is coincident with a pass word stored in the host computer 30.

Though an input of log-in data may be carried out in a user's office using the previously proposed non-portable data-communication terminal shown in Fig. 1, since, portable data-communication terminals are widely available, it is often possible to input log-in data from outside a user's office. However, in the previously proposed method illustrated in Fig. 1, any input of log-in data may be looked at secretly by a third party.

In addition, there is the problem with a portable

data-communication terminal that it may be stolen or lost, which was not a possibility with the previously proposed non-portable data-communication terminal.

In view of the above-mentioned problems, it is a feature of a method of authenticating a user and a system for carrying out the method to be described below by way of example in illustration of the invention, that they minimise the risk that a third party might use a portable data-communication terminal without the user's permission.

One method to be described below, by way of example in illustration of the invention, for use in authenticating a portable data-communication terminal user in a system which includes a portable data-communication terminal and a device for authenticating a user, each of which includes a transceiver for radio-communication with one another, includes the steps of (a) transmitting and receiving user-authentication data between the portable data-communication terminal and the user-authenticating device thereby to carry out a check as to whether the portable data-communication terminal is far away from the user-authenticating device by a distance equal to or smaller than a first distance within which the transceiver can make radio-communication between the portable data-communication terminal and the user-authenticating device, and (b) allowing the portable data-communication

terminal to carry out a predetermined operation only when the portable data-communication terminal is authenticated to be located within the first distance from the user-authenticating device.

It is preferable that the user-authentication data should be code data which is inherent to a user, and that the check is carried out by checking whether the user-authentication data of the portable data-communication terminal is coincident with the user-authentication data of the user-authenticating device.

It is also preferred that the portable data-communication terminal should have the function of logging in a host device by transmitting log-in data to the host device, and that the determination whether to allow the log-in of the portable data communication terminal to the host device should be in accordance with a result of the check.

The log-in data may be stored in advance in a memory in the portable data-communication terminal, and the log-in data may be read out from the memory, and transmitted to the host device.

For instance, the log-in data may be first data including an account name, used for identifying a user, and second data including a password, used for authenticating a user.

The check is preferably carried out only when a predetermined request is input to the portable data-communication terminal.

After the check has been carried out once, it may be repeatedly carried out after fixed intervals.

The portable data-communication terminal may transmit an authentication requesting signal, including data concerning a random number to the user-authenticating device, the user-authenticating device receiving the authenticating requesting signal may produce a response signal, including the data about the random number and authentication data stored in the user-authenticating device, and may transmit the thus produced response signal to the portable data-communication terminal, and the portable data-communication terminal receiving the response signal may extract the authentication data from the response signal, and compare the thus extracted authentication data with authentication data stored in the portable data-communication terminal.

A system for authenticating a user will also be described below, by way of example in illustration of the present invention, which includes (a) a portable terminal which provides data-communication and has a memory to store its own authentication data, and a radio-transceiver for making radio-communication for transmitting and receiving the authentication data, and (b) a device for authenticating a user, which includes a memory for storing authentication data of itself, and a radio-transceiver for providing radio-communication for transmitting and receiving the authentication data, the

portable data-communication terminal and the user-authenticating device transmitting and receiving the authentication data therebetween thereby to carry out a check as to whether the portable data-communication terminal is far away from the user-authenticating device by a distance equal to or smaller than a first distance within which the radio-transceivers can make radio-communication between the portable data-communication terminal and the user-authenticating device, the portable data-communication terminal being allowed to carry out a predetermined operation only when the portable data-communication terminal is determined to be located within the first distance from the user-authenticating device.

Preferably the user-authenticating device includes a radio-transmitter for transmitting authentication data of itself to the portable data-communication terminal by radio, and the portable data-communication terminal includes a radio-receiver for receiving the authentication data transmitted from the user-authenticating device, and a comparator to compare the thus received authentication data with the authentication data at the portable data-communication terminal.

The portable data-communication terminal may include a radio-transmitter to transmit a request for authentication to the user-authenticating device by radio, and the user-authenticating device may include a radio-receiver to receive the request transmitted from the portable data-communication terminal.

The portable data-communication terminal may include a timer which monitors whether the authentication data is received from the user-authenticating device within a predetermined period of time after the request has been transmitted to the user-authenticating device.

In one arrangement the portable data-communication terminal has the function of logging in a host device by transmitting log-in data to the host device, and includes a memory for storing the log-in data therein, and an access controller for transmitting the log-in data to the host device.

The portable data-communication terminal may include (a) a random number generator, (b) a comparative data producer which produces comparative data, based on the authentication data received from the memory and a random number transmitted from the random number generator, and transmits the thus produced comparative data to the comparator.

In one preferred arrangement the portable data-communication terminal includes a second timer for measuring a particular period of time after the portable data-communication terminal has been allowed to log-in to the host device, the check being carried out in each of the particular periods of time. The particular periods of time may be variable.

It is preferable that the radio-transmitter of the user-authentication device transmits a variable output for making radio-communication with the portable data-

communication terminal.

It is also preferred that the radio-transmitter of the portable data-communication terminal should transmit a variable output for making radio-communication with the user-authentication device.

In the above-mentioned arrangements illustrative of the present invention, the portable data-communication terminal and the user-authenticating device are used as a pair, and include means for making radio-communication between each other, that is, by means of a transceiver. The portable data-communication terminal and the user-authenticating device store authentication data therein, and it is checked to determine whether the portable data-communication terminal and the user-authenticating device are located within a distance within which the transceivers can make radio-communication between the portable data-communication terminal and the user-authenticating device, by transmitting and receiving the authentication data between the portable data-communication terminal and the user-authenticating device.

Only when it is recognized that the portable data-communication terminal and the user-authenticating device are located within the above-mentioned distance, is the portable data-communication terminal allowed to carry out a predetermined operation, for instance, the operation of logging-in to a host computer.

When it is not recognized that the portable data-communication terminal and the user-authenticating device

are located within the above-mentioned distance, it is judged that the portable data-communication terminal may be illegally used by a third party far from the user-authenticating device, and as a result, the portable data-communication terminal is prohibited from carrying out any operation. Hence, it is possible to prevent a third party from using the portable data-communication terminal without the user's permission.

Arrangements illustrative of the invention will now be described, by way of example, with reference to Figs. 2 to 5 of the accompanying drawings in which:-

Fig. 2 is a block schematic diagram of a system for authenticating a user,

Fig. 3 is a flow chart for use in illustrating the operation of a user-authenticating system illustrated in Fig. 2,

Fig. 4 is a flow chart for use in illustrating the operation of a portable data-communication terminal of the system illustrated in Fig. 2, and

Fig. 5 is a flow chart for use in illustrating the steps of user-authentication carried out in the system shown in Fig. 2.

Referring to the drawings, and first to Fig. 2, there is shown a user-authenticating device 10 and a portable data-communication terminal 20 operating together as a pair. Radio communication is provided between the user-authenticating device 10 and the portable data-communication terminal 20 for example, for

transmitting a log-in request from a user, or for accomplishing time management after certain periods of time by means of a timer, thereby to check whether the device 10 and the terminal 20 are within a distance within which they can make radio-communication. When it is judged that the user-authenticating device 10 and the portable data-communication terminal 20 are within such a distance, it is considered that the portable data-communication terminal 20 may be legally used. Only when the portable data-communication terminal 20 is judged to be legally usable is the portable data-communication terminal 20 is allowed to make access to a host computer 30.

The user-authenticating device 10 includes a radio-receiver 110, a response data producer 120, a radio-transmitter 130, and a user code memory 140.

The radio-receiver 110 receives a signal transmitted from the portable data-communication terminal 20, for requesting authentication to be carried out, extracts random number data out of the received authentication requesting signal, and transmits the extracted random number data to the response data producer 120.

The user code memory 140 stores a user code of the user-authenticating device 10, and transmits the user code to the response data producer 120.

The response data producer 120 produces response data, based on the random number data transmitted from the radio-receiver 110 and the user code transmitted from

the user code memory 140, and transmits the response data thus produced to the radio-transmitter 130.

The radio-transmitter 130 produces an authentication response signal, based on the response data transmitted from the response data producer 120, and transmits the authentication response signal thus produced to the portable data-communication terminal 20 by radio.

The portable data-communication terminal 20 includes an access controller 210, a random number generator 220, a radio-transmitter 230, a radio receiver 240, a user code memory 250, a comparative data producer 260, a data comparator 270, a log-in data memory 280, a first timer 290, a second timer 300, a communication controller 310, and an input section 320.

The access controller 210 controls the log-in and the log-out operations to the host computer 30 in response to a log-in request input through the input section 320.

The communication controller 310 controls the actual communication to the host computer 30.

The random number generator 220 generates a random number on receipt of an instruction transmitted from the access controller 210, and transmits the random number thus generated to the radio-transmitter 230 and the comparative data producer 260.

The radio-transmitter 230 produces an authentication requesting signal, based on the random number transmitted from the random number generator 220, and transmits the

authentication requesting signal to the user-authenticating device 10 by radio.

The radio-receiver 240 receives the authentication response signal transmitted from the user-authenticating device 10, extracts the response data from the received authentication response signal, and transmits the response data thus extracted to the data comparator 270.

The user code memory 250 stores the same user code as the user code stored in the user-authenticating device 10. The user code memory 250 transmits the user code to the comparative data producer 260.

The comparative data producer 260 produces comparative data, based on the random number transmitted from the random number generator 220 and the user code transmitted from the user code memory 250, and transmits the comparative data thus produced to the data comparator 270.

The data comparator 270 compares the comparative data transmitted from the comparative data producer 260 to the response data transmitted from the radio-receiver 240, and transmits the result of the comparison to the access controller 210.

The second timer 300 starts counting the time immediately after the access controller 210 has provided an instruction to the random number generator 220. When the authentication response signal is not received after the lapse of a certain period of time, the second timer 300 informs the access controller 210 that there is a

time-out situation.

The log-in data memory 280 stores the data necessary for the portable data-communication terminal to log-in to the host computer 30, and transmits the log-in data to the access controller 210 in response to a request transmitted from the access controller 210.

The first timer 290 starts counting the time just after the log-in of the portable data-communication terminal 20 to the host computer 30 has been approved, and counts a certain period of time, in which a user-authenticating operation, which has been carried out when log-in of the portable data-communication terminal 20 to the host computer 30 has been approved, is carried out. When the time is out or expired, that is, when a user is not authenticated within such a certain period of time, the first timer 290 informs the access controller 210 that there is a time-out situation.

In response, the access controller 210 receives the result of the comparison from the data comparator 270. If the result shows that the comparative data is coincident with the response data, the access controller 210 reads the information, necessary for the portable data-communication terminal 20 to log-in, to the host computer 30 out of the log-in data memory 280, and transmits the thus read-out log-in data to the communication controller 310. As a result, the portable data-communication terminal 20 is logged-in to the host computer 30.

When the result shows that the comparative data is not coincident with the response data, or when the second timer 300 informs the access controller 210 that there is a time-out situation, the access controller 210 judges that a user is not authenticated, and transmits a request for disconnection to the communication controller 310. The connection to the host computer 30 is then interrupted.

The interval during which a user authentication is carried out by means of the first timer 290 may be determined, as desired. For instance, the interval may, for example, be set to be equal to about 10 seconds, in order to avoid the risk that others may use the portable data-communication terminal 20 while a user having the user-authenticating device 10 is away from the portable data-communication terminal 20. However, since such a risk is dependent on users, the interval may, for example, be set to be equal to about 1 minute, if such a risk is relatively low.

The interval may be varied according to an operation carried out by a user.

A distance within which the radio-transmitters 130 and 230 and the radio-receivers 110 and 240 can make radio-communication therebetween is dependent to some extent upon a user's circumstance. For instance, such a distance may be set within the range of a couple of meters to tens of meters.

The radio-transmitter 130 of the user-authenticating

device 10 may be designed to be able to transmit a variable output so that a user can select a desired output. Additionally or as an alternative, the radio-transmitter 230 of the portable data-communication terminal 20 may be designed in the same manner.

A signal format in the data-communication to be carried out in the embodiment being described is in accordance with the standard specification (RCRSTD-27, 28), such as the standard specification for a PDC type cellular phone and personal handy phone system (PHS). However, it should be noted that various signal formats may be used in dependence upon the infrastructure of an area in which the system is employed.

A longer user code would ensure higher security. In the system of authenticating a user in the arrangement being described, a user code is not allowed to overlap other user codes. However, a user code which is too long would take a long time for carrying out the calculation. Hence, a user code is preferably designed to have a length sufficient to avoid overlapping other user codes, even if the portable data-communication terminal 20 is widely used. For instance, a user code may be designed to have 64 digits in binary numerals.

The user code memories 140 and 250 storing such a user code may have a read only memory (ROM).

A process for authenticating data in the particular system being described is explained below with reference to Figs. 3 to 5.

In particular, Fig. 4 shows the operation of the access controller 210, and Fig. 5 shows the operation of user authentication to be carried out between the user-authenticating device 10 and the portable data-communication terminal 20.

With reference to Fig. 3, when the user-authenticating device 10 is turned on, the user-authenticating device 10 is initially in a stand-by condition, that is, it is waiting for an authentication-requesting signal to be transmitted from the portable data-communication terminal 20. The radio-receiver 110 checks whether an authentication-requesting signal is received or not in step S201.

If not (S202), the radio-receiver 110 repeats the check to establish whether an authentication-requesting signal has been received, in step S203.

If an authentication requesting signal has been received (S204), the radio-receiver 110 extracts a random number from the received authentication requesting signal in step S205, and transmits the random number thus extracted to the response data producer 120 in step S206.

The response data producer 120 reads a user code out of the user code memory 140 in step S207, produces response data, based on the random number and the user code thus read-out in step S208, and transmits the thus produced response data to the radio-transmitter 130, in step S209.

The radio-transmitter 130 produces an authentication

response signal, based on the response data transmitted from the response data producer 120, in step S210, and transmits the authentication response signal thus produced to the portable data-communication terminal 20 by radio, in step S211.

Thereafter, the user-authenticating device 10 is again put into a stand-by condition, namely, a condition of waiting for the receipt of an authentication requesting signal transmitted from the portable data-communication terminal 20, in step S203.

With reference to Fig. 4, when the portable data-communication terminal 20 is turned on, the portable data-communication terminal 20 is initially in a stand-by condition, that is, in a condition of waiting for a log-in request to be input through the input section 320. The access controller 210 checks whether a log-in request has been input through the input section 320, in step S303.

If a log-in request has been input (step S304), the portable data-communication terminal 20 checks whether a user authentication has already been carried out, in step S400, and then, checks the result of the user authentication, which was conducted by the communication between the user-authenticating device 10 and the portable data-communication terminal 20, in step S305.

The process of carrying out user authentication (step S400) will be explained later with reference to Fig. 5.

If a user is not authenticated (S306), the portable data-communication terminal 20 is again put into a stand-by condition (S303).

If a user is authenticated (S307), the access controller 210 reads log-in data out of the log-in data memory 280 in step S308, and transmits the log-in data to the communication controller 310 in step S309.

Receiving the log-in data from the access controller 210, the communication controller 310 causes the portable data-communication terminal 20 to log-in to the host computer 30, in step S310.

After the portable data-communication terminal 20 has been logged-in to the host computer 30, the access controller 210 starts operating the first timer 290, in step S312. Then, the access controller 210 is in a condition of waiting for a time-out situation until the next user-authentication is carried out, and checks whether time is out, or not, in step S314.

If time is not out (S315), the access controller 210 checks whether a log-out request has been input through the input section 320 in step S317. If a log-out request has not been input (S318), a check, as to whether time is out (S314), is carried out again (S313). If a log-out request is input through the input section 320 in step S319, the operation of the first timer 290 is stopped, in step S320. Then, the same procedure as the procedure which is to be carried out when a user is not authenticated is carried out (S324).

When the time is out in the first timer 290 in step S316, user authentication is carried out again in steps 400 and 321.

If a user is authenticated (S322), the steps S311 to S321 are repeated.

If a user is not authenticated (S323), the access controller 210 transmits a request for interruption to the communication controller 310, in step S325. The communication controller 310 causes the portable data-communication terminal 20 to be logged-out from the host computer 30, in step S326.

Then, the portable data-communication terminal 20 is again put in the stand-by condition, that is, in a condition of waiting for a log-in request to be input through the input section 320 (step S303).

The procedure for user authentication will now be explained with reference to Fig. 5.

First, the access controller 210 instructs the random number generator 220 to generate a random number, and then transmit the random number thus generated to the radio-transmitter 230, in step S401.

The radio-transmitter 230 produces an authentication requesting signal, based on the random number transmitted from the random number generator 220, in step S402, and then, transmits the authentication requesting signal thus produced by radio to the radio-receiver 110 of the user-authenticating device 10, in step S403.

After the authentication requesting signal has been

transmitted, the access controller 210 starts the second timer 300 into operation, in step S404, which measures a certain period of time during which the portable data-communication terminal 20 waits to receive the authentication response signal.

While the portable data-communication terminal 20 is in the stand-by condition, the radio-receiver 240 checks whether an authentication response signal has been received or not, in step S406.

If an authentication response signal has not been received (S407), the second timer 300 is checked in order to establish whether time is out, in step S409. If time is not out (S410), a check to establish whether an authentication response signal has been received or not is repeated (S405).

If an authentication response signal has been received (S408), the radio-receiver 240 extracts response data from the received authentication response signal, in step S414, and transmits the response data to the data comparator 270, in step S415.

The comparative data producer 260 produces comparative data in step S418, based on the random number transmitted from the random number generator 220 (step S416) and the user code read out of the user code memory 250 (S417), and transmits the comparative data thus produced to the data comparator 270, in step S419.

The data comparator 270 compares the response data transmitted from the radio-receiver 240 to the

comparative data transmitted from the comparative data producer 260, in step S420. If they are coincident with each other (S422), the data comparator 270 judges that a user is authenticated (S423). If they are not coincident with each other (S421), the data comparator 270 judges that a user is not authenticated (S413).

After the step of user-authentication has been finished, the second timer 300 is stopped in step S425. Thus, the procedure of user-authentication is finished in step S426.

When time is out in the second timer 300 (S411), there is carried out the same procedure as the procedure which is carried out when the comparative data is not coincident with the response data, in step S412.

In the particular arrangement being described, a user is not allowed to have access to the host computer 30, unless the user has both the user-authenticating device 10 and the portable data-communication terminal 20. Hence, it is possible to prevent a third party from making illegal access to the host computer 30, even if the portable data-communication terminal 20 is stolen or lost.

In addition, since user-authentication can be carried out via radio-communication between the user-authenticating device 10 and the portable data-communication terminal 20, it is not necessary for the user-authenticating device 10 and the portable data-communication terminal 20 actually to make contact with

each other. Hence, a user may have one of the authenticating device 10 and the terminal 20 separately, which ensures that there is less possibility of the portable data-communication terminal 20 being lost or stolen.

Furthermore, since user-authentication is carried out via radio-communication, a user is not authenticated if the user-authenticating device 10 and the portable data-communication terminal 20 are far away from each other. Hence, even if a user having the user-authenticating device 10 with him is temporarily away from the portable data-communication terminal 20, it would be possible to prevent a third party from having access to the host computer 30 from the portable data-communication terminal 20, thereby ensuring an enhancement in security.

In addition, the content of a radio-communication for use in carrying out the user-authentication may be varied each time, as a result of the use of a random number, which ensures protection from the data being tapped during the radio-communication.

In the system being described, since the log-in data stored in the log-in data memory 280 is read out each time that a user-authentication is carried out, it is no longer necessary for a user to input log-in data each time that a user-authentication is carried out. Hence, even if the portable data-communication terminal 20 is used outside a user's office to log-in to the host

computer 30, it is possible to prevent log-in data from being stolen comparatively easily.

In addition, it is possible to shorten the time necessary for carrying out the step of authentication, and to simplify the procedure for carrying out the authentication.

The above-mentioned arrangement has been described as an example wherein the log-in operation of the portable data-communication terminal 20 to the host computer 30 is restricted to being carried out in dependence upon the result of a user-authentication. However, it should be noted that other operations may be restricted to being carried out, in dependence upon the result of a user-authentication.

It will be understood that, although particular arrangements have been described, by way of example, in illustration of the invention, variations and modifications thereof, as well as other arrangements may be made within the scope of the protection sought by the appended claims.

CLAIMS

1. A method of authenticating a portable data-communication terminal user in a system which includes a portable data-communication terminal and a device for authenticating a user, the terminal and the device each including a transceiver for effecting radio-communication therebetween, the method including the steps of:-

(a) transmitting and receiving user-authentication data between the portable data-communication terminal and the user-authenticating device thereby to carry out a check to determine whether the portable data-communication terminal is at a distance from the user-authenticating device which is equal to or smaller than a first distance within which the transceiver is able to make radio-communication between the portable data-communication terminal and the user authenticating device, and

(b) allowing the portable data-communication terminal to carry out a predetermined operation only when it has been determined that the portable data-communication terminal is located within the first distance from the user-authenticating device.

2. A method as claimed in claim 1, wherein the user-authentication data is code data inherent to a user, and wherein the check is carried out by checking whether

user-authentication data of the portable data-communication terminal is coincident with user-authentication data of the user-authenticating device.

3. A method as claimed in either claim 1 or claim 2, wherein the portable data communication terminal logs-in to a host device by transmitting log-in data to the host device, and wherein the logging-in of the portable data-communication terminal to the host device is allowed according to the result of the check.

4. A method as claimed in claim 3, wherein log-in data is stored in advance in a memory in the portable data-communication terminal, and the log-in data is read out of the memory, and transmitted to the host device.

5. A method as claimed in claim 3, wherein the log-in data includes first data including account data, used for identifying a user, and second data including a password, used for authenticating a user.

6. A method as claimed in either claim 1 or claim 2, wherein the check is carried out only when a predetermined request is input into the portable data-communication terminal.

7. A method as claimed in claim 6, wherein after the check has been carried out once, the check is

repeated after a fixed interval of time.

8. A method as claimed in either claim 1 or claim 2, wherein the portable data-communication terminal transmits an authentication requesting signal including random number data to the user-authenticating device, the user-authenticating device receives the authenticating requesting signal and produces a response signal, including the random number data and authentication data stored in the user-authenticating device, and transmits the response signal thus produced to the portable data-communication terminal, and the portable data-communication terminal receives the response signal, extracts the authentication data from the response signal, and compares the authentication data thus extracted with authentication data stored in the portable data-communication terminal.

9. A system for authenticating a user which includes

(a) a portable terminal for providing data-communication, the portable terminal having a memory for storing authentication data, and a radio-transceiver for carrying out radio-communication, including transmitting and receiving authentication data, and

(b) a device which authenticates a user, including a memory for storing authentication data, and a radio-transceiver for carrying out radio-communication,

including transmitting and receiving the authentication data,

the portable data-communication terminal and the user-authenticating device providing means for transmitting and receiving the authentication data therebetween, thereby to carry out a check to determine whether the portable data-communication terminal is at a distance from the user-authenticating device which is equal to or smaller than a first distance within which the radio-transceivers can make radio-communication between the portable data-communication terminal and the user-authenticating deice, the portable data-communication terminal being allowed to carry out a predetermined operation only when the portable data-communication terminal is determined to be located within the first distance from the user-authenticating device.

10. A system as claimed in claim 9, wherein the user-authenticating device includes a radio-transmitter for transmitting authentication data to the portable data-communication terminal by radio, and wherein the portable data-communication terminal includes a radio-receiver for receiving the authentication data transmitted from the user-authenticating device, and a comparator for comparing the authentication data thus received with the authentication data of the portable data-communication terminal.

11. A system as claimed in claim 10, wherein the portable data-communication terminal includes a radio-transmitter for transmitting a request for authentication to the user-authenticating device by radio, and wherein the user-authenticating device includes a radio-receiver for receiving the request transmitted from the portable data-communication terminal.

12. A system as claimed in claim 11, wherein the portable data-communication terminal includes a timer which monitors whether authentication data has been received from the user-authenticating device within a predetermined period of time after the request has been transmitted to the user-authenticating device.

13. A system as claimed in any one of claims 9, 10 or 11, wherein the portable data-communication terminal logs-in to a host device by transmitting log-in data to the host device, and includes a memory for storing the log-in data therein, and an access controller for transmitting the log-in data to the host device.

14. A system as claimed in any one of claims 10, 11 or 12, wherein the portable data-communication terminal includes

(a) a random number generator, and

(b) a comparative data producer which produces comparative data, based on the authentication data

received from the memory, means for transmitting a random number from the random number generator, and means for transmitting the comparative data thus produced to the comparator.

15. A system as claimed in claim 13, wherein the portable data-communication terminal includes a second timer for measuring a certain period of time after the portable data-communication terminal has been allowed to log-in to the host device, the check being carried out after the certain period of time.

16. A system as claimed in claim 15, wherein the certain period of time is variable.

17. A system as claimed in any one of claims 10, 11 or 12, wherein the radio-transmitter of the user-authentication device includes means for transmitting a variable output for making radio-communication with the portable data-communication terminal.

18. A system as claimed in either claim 11 or 12, wherein the radio-transmitter of the portable data-communication terminal includes means for transmitting a variable output for making radio-communication with the user-authentication device.

19. A method of authenticating a portable data-

communication terminal user as claimed in claim 1, substantially as described herein with reference to Figures 2 to 5 of the accompanying drawings.

20. A system for authenticating a user as claimed in claim 9, substantially as described herein with reference to Figures 2 to 5 of the accompanying drawings.